S03P1318 US00

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１１月１５日

出 願 番 号
Application Number: 特願２００２－３３１６７７

[ST. 10/C]: [ＪＰ２００２－３３１６７７]

出 願 人
Applicant(s): ソニー株式会社

２００３年 ８月２５日

特許庁長官
Commissioner,
Japan Patent Office 今 井 康 夫

出証番号 出証特２００３－３０６９４１７

【書類名】　特許願
【整理番号】　0290507703
【提出日】　平成14年11月15日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/31
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　菅　真紀子
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100094053
　【弁理士】
　【氏名又は名称】　佐藤　隆久
【手数料の表示】
　【予納台帳番号】　014890
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9707389
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　回路構成方法、その装置およびそのプログラム

【特許請求の範囲】

【請求項１】

所定のデータに対してそれぞれ異なる複数の第１の演算を施す演算回路の回路設計方法であって、

前記複数の第１の演算のそれぞれを構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する第１の工程と、

前記複数の第１の演算で共用され前記第１の工程で特定された前記第２の演算を行う第１の演算回路と、前記複数の第１の演算のそれぞれを構成する前記複数の第２の演算のうち前記第１の工程で特定された前記第２の演算以外の演算を行う第２の演算回路とからなる前記演算回路を構成する第２の工程と

を有する回路構成方法。

【請求項２】

前記第１の演算は、線形変換の演算であり、

前記第２の演算は、加算である

請求項１に記載の回路構成方法。

【請求項３】

前記複数の第１の演算が、前記所定のデータに対して第１の線形変換をそれぞれ異なる所定の回数施す演算である場合に、

前記複数の第１の演算のそれぞれについて、前記所定の回数に対応する数の前記第１の線形変換を合成した第２の線形変換を規定する第３の工程

をさらに有し、

前記第１の工程において、前記第３の工程で前記複数の第１の演算のそれぞれについて規定された前記第２の線形変換を構成する前記複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する

請求項１に記載の回路構成方法。

【請求項４】

前記第２の工程において、前記第３の工程で規定された前記第２の線形変換を

基に、前記所定のデータに対して前記複数の第１の演算を並列に行うように前記演算回路を構成する

請求項３に記載の回路構成方法。

【請求項５】

前記所定データは、所定の線形空間上の所定の基底により、ベクトルで表現されたものであり、

前記線形変換は、前記線形空間上で規定された変換である

請求項３に記載の回路構成方法。

【請求項６】

前記所定の線形空間を下記（１－１）で示し、前記所定の基底として下記（１－２）に示す基底を用い、下記（１－２）に示す基底を基に前記所定のデータであるデータａが下記（１－３）のように示されるとき、当該データａをｍ次元ベクトルとして下記（１－４）で示し、前記第１の線形変換を下記（１－１）に示す線形空間上の線形変換Ｄとし、前記複数の演算の結果であるデータｂをｋ次元ベクトルとして下記（１－５）で示し、下記（１－５）に示すデータｂを構成する各演算の結果を示すデータｂｉをｄｉ次元ベクトルとして下記（１－６）で示した場合に

前記第３の工程において、ｄｉ行ｍ列の行列Ｄで構成され前記第２の線形変換を行う下記（１－７）で示される行列Ｍを規定し、

前記第１の工程において、前記第３の工程で規定された下記（１－７）を基に、前記複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する

請求項３に記載の回路構成方法。

ここで、ｍ，ｄｉは２以上の整数であり、前記複数の演算の少なくとも一つに対応する前記所定の回数が２以上であり、ｋは２以上の整数である。

【数１】

$$\text{線形空間}\quad F_{g^m} \qquad (1-1)$$

【数２】

$$\{\gamma_1, \gamma_2, \cdots, \gamma_m\} \qquad (1-2)$$

【数３】

$$a = a_1 \gamma_1 + a_2 \gamma_2 + \cdots + a_m \gamma_m \qquad (1-3)$$

【数４】

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} \qquad (1-4)$$

【数５】

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} \qquad (1-5)$$

【数６】

$$b_i = \begin{pmatrix} b_{i,1} \\ b_{i,2} \\ \vdots \\ b_{i,di} \end{pmatrix} \qquad (1-6)$$

【数７】

$$M = \begin{pmatrix} D \\ D^2 \\ \vdots \\ D^K \end{pmatrix} \qquad (1-7)$$

【請求項７】

前記所定の基底として下記（１－８）に示す基底を用い、前記データａが下記（１－９）のように示されるとき、前記データａをｍ次元ベクトルとして下記（１－１０）の示す

請求項６に記載の回路構成方法。

【数８】

$$\{1, \gamma, \gamma^2, \cdots, \gamma^{m-1}\} \qquad (1-8)$$

【数９】

$$a = a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3 + \cdots + a_{m-1}\gamma^{m-1} \qquad (1-9)$$

【数１０】

$$a = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{m-1} \end{pmatrix} \qquad (1-10)$$

【請求項８】

前記第３の工程において、前記線形空間上の元γを基にγ^r倍の演算を行う前記行列Ｄで構成された前記行列Ｍを規定する

請求項６に記載の回路構成方法。

【請求項９】

所定のデータに対してそれぞれ異なる複数の第１の演算を施す演算回路の回路設計装置であって、

前記複数の第１の演算のそれぞれを構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する第１の手段と、

前記複数の第１の演算で共用され前記第１の手段で特定された前記第２の演算を行う第１の演算回路と、前記複数の第１の演算のそれぞれを構成する前記複数の第２の演算のうち前記第１の手段で特定された前記第２の演算以外の演算を行う第２の演算回路とからなる前記演算回路を構成する第２の手段と

を有する回路構成装置。

【請求項１０】

所定のデータに対してそれぞれ異なる複数の第１の演算を施す演算回路の回路設計装置で実行されるプログラムであって、

前記複数の第１の演算のそれぞれを構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する第１の手順と、

前記複数の第１の演算で共用され前記第１の手順で特定された前記第２の演算を行う第１の演算回路と、前記複数の第１の演算のそれぞれを構成する前記複数

の第２の演算のうち前記第１の手順で特定された前記第２の演算以外の演算を行う第２の演算回路とからなる前記演算回路を構成する第２の手順と

を有するプログラム。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】

本発明は、例えば、誤り訂正符号や復号などを行う場合に用いられる線形変換などの演算を行う演算回路の回路構成方法、その装置およびそのプログラムに関する。

【０００２】

【従来の技術】

例えば、ハミング符号などの誤り訂正符号や復号では、有限体上で規定された線形空間で種々の線形変換の演算が行われる。

このような線形変換の演算は、例えば、線形空間上の所定の基底により、線形空間上の元をベクトルで表現し、このベクトルに対して線形変換の演算を施して新たなベクトルを得る。

上述した誤り訂正符号や復号では、例えば、複数ビットの所定データに対してそれぞれ異なる線形変換の複数の演算を行なう場合がある。

従来では、例えば、上記複数の演算をそれぞれ独立して行なうように演算回路を構成（設計）している。

【０００３】

【発明が解決しようとする課題】

しかしながら、上述したように、上記複数の演算をそれぞれ独立して行なうように演算回路を構成すると、演算回路が大規模になるという問題がある。

【０００４】

本発明は上述した従来技術の問題点に鑑みてなされ、所定データに対してそれぞれ異なる複数の演算を行なう演算回路を構成する場合に、当該演算回路を小規模に構成できる回路構成方法、その装置およびそのプログラムを提供することを目的とする。

【０００５】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第１の発明の回路設計方法は、所定のデータに対してそれぞれ異なる複数の第１の演算を施す演算回路の回路設計方法であって、前記複数の第１の演算のそれぞれを構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する第１の工程と、前記複数の第１の演算で共用され前記第１の工程で特定された前記第２の演算を行う第１の演算回路と、前記複数の第１の演算のそれぞれを構成する前記複数の第２の演算のうち前記第１の工程で特定された前記第２の演算以外の演算を行う第２の演算回路とからなる前記演算回路を構成する第２の工程とを有する。

【０００６】

第１の発明の回路構成方法では、先ず、第１の工程において、複数の第１の演算のそれぞれを構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算が特定される。

そして、第２の工程において、前記複数の第１の演算で共用され前記第１の工程で特定された前記第２の演算を行う第１の演算回路と、前記複数の第１の演算のそれぞれを構成する前記複数の第２の演算のうち前記第１の工程で特定された前記第２の演算以外の演算を行う第２の演算回路とからなる前記演算回路が構成される。

【０００７】

第２の発明の回路構成装置は、所定のデータに対してそれぞれ異なる複数の第１の演算を施す演算回路の回路設計装置であって、前記複数の第１の演算のそれぞれを構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する第１の手段と、前記複数の第１の演算で共用され前記第１の手段で特定された前記第２の演算を行う第１の演算回路と、前記複数の第１の演算のそれぞれを構成する前記複数の第２の演算のうち前記第１の手段で特定された前記第２の演算以外の演算を行う第２の演算回路とからなる前記演算回路を構成する第２の手段とを有する。

【０００８】

第２の発明の回路構成装置では、第１の手段が、複数の第１の演算のそれぞれを構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する。

そして、第２の手段が、前記複数の第１の演算で共用され前記第１の手段で特定された前記第２の演算を行う第１の演算回路と、前記複数の第１の演算のそれぞれを構成する前記複数の第２の演算のうち前記第１の手段で特定された前記第２の演算以外の演算を行う第２の演算回路とからなる前記演算回路を構成する。

【０００９】

第３の発明のプログラムは、所定のデータに対してそれぞれ異なる複数の第１の演算を施す演算回路の回路設計装置で実行されるプログラムであって、前記複数の第１の演算のそれぞれを構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する第１の手順と、前記複数の第１の演算で共用され前記第１の手順で特定された前記第２の演算を行う第１の演算回路と、前記複数の第１の演算のそれぞれを構成する前記複数の第２の演算のうち前記第１の手順で特定された前記第２の演算以外の演算を行う第２の演算回路とからなる前記演算回路を構成する第２の手順とを有する。

【００１０】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

〔本発明の関連技術〕

図１は、本発明の関連技術に係わる演算回路１０１の構成図である。

演算回路１０１は、データａを入力として、データb_1～b_kを出力する。

演算回路１０１は、ｉを$1 \leqq i \leqq k$を満たす２以上の自然数、l_iを自然数とした場合に、各系統で行列$M_{i,1}$～M_{i,l_i}によって規定された演算$C_{i,1}$～C_{i,l_i}を順に行う複数系統の演算回路モジュールを有し、これらの演算回路モジュールで並列に演算を行う。

各演算モジュールは、演算$C_{i,1}$～C_{i,l_j}をそれぞれ行う複数の演算回路２ｉl_jを直接に接続して構成される。

演算回路１０１は、線形空間上の基底によりベクトル表現されたデータａを入力し、演算回路２１ｌ$_1$～２ｋｌ$_k$でデータａに線形演算を施し、演算回路２１ｌ$_1$～２ｋｌ$_k$からそれぞれｂ$_1$～ｂ$_k$を出力する。

【００１１】

図１に示す演算回路１は、各演算回路モジュール内の演算$C_{i,1}$～$C_{i,li}$を図２に示すように合成した演算回路モジュールｉｌ$_j$（ｊは２以上の整数）を用いた演算回路２０１のように構成することで、小規模化および高速化が図れる。

この場合に、図２および下記（２－１）に示すように規定された線形変換列が、下記（２－２）に示すように合成される。

【００１２】

【数１１】

$$\{C_{1,1},\ C_{1,2},\ \cdots\ C_{1,l_1}\},$$
$$\{C_{2,1},\ C_{2,2},\ \cdots\ C_{2,l_2}\},$$
$$\cdots\ \cdots\ \cdots\ \cdots \qquad (2\text{-}1)$$
$$\{C_{k,1},\ C_{k,2},\ \cdots\ C_{k,l_k}\},$$

$$\{C_{i,j-1}\text{の値域}\} \subset \{C_{i,j}\text{の定義域}\}$$

【００１３】

【数１２】

$$C_{1,l_1} \circ \cdots \circ C_{1,2} \circ C_{1,1} : a \mapsto b_1$$
$$C_{2,l_2} \circ \cdots \circ C_{2,2} \circ C_{2,1} : a \mapsto b_2 \qquad (2\text{-}2)$$
$$\cdots$$
$$C_{k,l_k} \circ \cdots \circ C_{k,2} \circ C_{k,1} : a \mapsto b_k$$

【００１４】

このとき、上記（２－１）に示す演算$C_{i,1}$～$C_{i,li}$を線形変換を行う行列$M_{i,1}$～$M_{i,li}$とすると、上記（２－１），（２－２）は、それぞれ下記（２－３），（２－４）のように示される。

【００１５】

【数１３】

$$\begin{aligned}&\{M_{1,1},\ M_{1,2},\cdots\ M_{1,l_1}\},\\&\{M_{2,1},\ M_{2,2},\cdots\ M_{2,l_2}\},\\&\cdots\ \cdots\ \cdots\ \cdots\\&\{M_{k,1},\ M_{k,2},\cdots\ M_{k,l_k}\},\end{aligned}\qquad (2-3)$$

【００１６】

【数１４】

$$\begin{aligned}&M_1 := M_{1,l_1},\ \cdots\ M_{1,2}M_{1,1} : a \mapsto b_1\\&M_2 := M_{2,l_2},\ \cdots\ M_{2,2}M_{2,1} : a \mapsto b_2\\&\cdots\\&M_k := M_{k,l_k},\ \cdots\ M_{k,2}M_{k,1} : a \mapsto b_k\end{aligned}\qquad (2-4)$$

【００１７】

これにより、演算回路２０１を、下記（２－５）に示す行列を行う回路として構成できる。

【００１８】

【数１５】

$$M := \begin{pmatrix} M_1 \\ M_2 \\ \cdots \\ M_k \end{pmatrix} : a \mapsto \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_k \end{pmatrix} \qquad (2-5)$$

【００１９】

次に、入力したデータＦＳ０に対して、第１の線形変換Ｄをそれぞれ異なる所定の回数施す複数の演算を行い、当該演算の結果であるデータb_1～b_kを出力する演算回路の構成方法について説明する。

図３は、このような演算回路３０１、並びにその周辺回路を説明するための図である。

【００２０】

図３に示すように、セレクタ３１２において選択信号ＳＥＬを基に、入力データａとデータＭＬＳとのうち一方のデータが選択され、当該選択されたデータＦＳ０がレジスタ313_0および演算回路３０１に出力される。

演算回路３０１は、セレクタ１２から入力したデータＦＳ０に対して、第１の線形変換Ｄをそれぞれ異なる所定の回数施す複数の演算を行い、当該演算の結果であるデータb_1～b_kをそれぞれレジスタ313_1～313_kに出力する。

レジスタ313_0～313_kは、入力したデータＦＳ０，b_1～b_kを保持し、所定のタイミングで、これらをデータOUT_0～OUT_Kとして出力する。

演算回路３１４は、データOUT_kを入力し、これに第１の線形演算Ｄを施して、その結果であるデータＭＳＬをセレクタ３１２に出力する。

【００２１】

演算回路３０１は、例えば、図３に示すように、それぞれ線形変換Ｄを行う複数の演算回路321_1～321_kを直列に接続し、データａを初段の回路321_1に入力し、個々の演算回路321_1～321_kで生成されたデータb_1～b_kをレジスタ313_1～313_kに出力するように構成（設計）される。

【００２２】

ここで、図３に示す演算回路３０１は、有限体Ｆ（2^4）の元、α，$\alpha^2+\alpha+1=0$に対してα倍演算を行なうものである場合、図４に示すように構成される。

この場合に、図３に示すように、あるタイミングで入力されたデータａに対して、データOUT_0，OUT_1，OUT_2は、以下のようになる。

【００２３】

【表１】

OUT_0：a，$a\times\alpha^{k+1}$，$a\times\alpha^{2k+2}$，・・・，

OUT_1：　$a\times\alpha$，$a\times\alpha^{K+2}$，$a\times\alpha^{2K+3}$，・・・，

OUT_2：　$a\times\alpha^2$，$a\times\alpha^{K+3}$，$a\times\alpha^{2K+4}$，・・・，

【００２４】

ここで、ＦＳ０＝Ａ０＋Ａ１αとすると、以下のようになる。

$FS0\cdot\alpha=A1+(A0+A1)\alpha$

$FS0\cdot\alpha^2=(A0+A1)+A0\alpha$

【００２５】

従って、図４に示す演算回路321_1，321_2は、図５に示すように、それ

ぞれ１個の加算回路３５１$_1$，３５１$_2$によって構成される。

〔００２６〕

しかしながら、上述したように、演算回路３０１を設計すると、回路規模が大きくなるという問題がある。

また、演算回路３０１において、データａを初段の回路３２１$_1$に入力してから最終段の回路３２１$_k$からデータｂ$_k$が出力されるまでの時間が長くなり、高性能な演算回路３０１を設計できないという問題がある。

〔００２７〕

以下、上述した関連技術の問題点を解決する本発明の実施形態を説明する。

〔第１実施形態〕

図６は、本実施形態の回路構成方法で構成（設計）される演算回路１１の周辺回路を説明するための図である。

図６に示すように、セレクタ１２において選択信号ＳＥＬを基に、入力データａとデータＭＬＳとのうち一方のデータが選択され、当該選択されたデータＦＳ０がレジスタ１３$_0$および演算回路１１に出力される。

演算回路１１は、セレクタ１２から入力したデータＦＳ０に対して、第１の線形変換Ｄをそれぞれ異なる所定の回数施す複数の演算を行い、当該演算の結果であるデータｂ$_1$～ｂ$_k$をそれぞれレジスタ１３$_1$～１３$_k$に出力する。

レジスタ１３$_0$～１３$_k$は、入力したデータＦＳ０，ｂ$_1$～ｂ$_k$を保持し、所定のタイミングで、これらをデータＯＵＴ$_0$～ＯＵＴ$_K$として出力する。

演算回路１４は、データＯＵＴ$_k$を入力し、これに第１の線形演算Ｄを施して、その結果であるデータＭＳＬをセレクタ１２に出力する。

〔００２８〕

本実施形態の回路構成方法は、図６に示す演算回路１１を構成（設計）するものである。

〔００２９〕

本実施形態では、所定の線形空間が、ｑを素数とした場合に有限体Ｆ$_q$のｍ次拡大であり、その元がＦ$_q$上のｍ次ベクトルで表現された場合に、当該所定の線形空間を下記（３－１）、あるいはＦ（ｑ^m）で示す。

【００３０】

【数１６】

$$\text{線形空間}\quad F_g{}^m \tag{3-1}$$

【００３１】

また、所定の基底として下記（３－２）に示す基底を用い、下記（３－２）に示す基底を基に前記所定のデータであるデータａを下記（３－３）のように示す。

【００３２】

【数１７】

$$\{\gamma_1, \gamma_2, \cdots, \gamma_m\} \tag{3-2}$$

【００３３】

【数１８】

$$a = a_1\gamma_1 + a_2\gamma_2 + \cdots + a_m\gamma_m \tag{3-3}$$

【００３４】

また、上記データａをｍ次元ベクトルとして下記（３－４）のように示す。

【００３５】

【数１９】

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} \tag{3-4}$$

また、上記第１の線形変換Ｄを上記（３－１）に示す線形空間上の線形変換Ｄとする。

【００３６】

また、上記複数の演算の結果であるデータｂをｋ次元ベクトルとして下記（３－５）で示し、下記（３－５）に示すデータｂを構成するの各演算の結果を示すデータｂｉをｄｉ次元ベクトルとして下記（３－６）で示す。

ここで、ｍ，ｄｉは２以上の整数であり、前記複数の演算の少なくとも一つに

対応する前記所定の回数が２以上であり、ｋは２以上の整数である。

【００３７】

【数２０】

$$\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} \qquad (3-5)$$

【００３８】

【数２１】

$$\mathbf{b}_i = \begin{pmatrix} b_{i,1} \\ b_{i,2} \\ \vdots \\ b_{i,d_i} \end{pmatrix} \qquad (3-6)$$

【００３９】

ここで、上記複数の演算を、それぞれＯＰ$_1$ ～ＯＰ$_K$ とすると、これらは下記（３－７）で示される。

【００４０】

【数２２】

$$\begin{array}{llll} OP_1: & \{D\}, & D: & a \mapsto b_1 \\ OP_2: & \{D,\ D\}, & D^2 := D \circ D: & a \mapsto b_2 \\ OP_3: & \{D,\ D,\ D\}, & D^3 := D \circ D \circ D: & a \mapsto b_2 \\ & \cdots\ \cdots\ \cdots\ \cdots\ \cdots & \cdots & \\ OP_k: & \{D,\ D,\ D,\ \cdots, D\}, & D^k := D \circ D \circ D \circ \cdots \circ D: & a \mapsto b_k \end{array} \qquad (3-7)$$

【００４１】

そして、第１の線形変換Ｄを表すｄｉ行ｍ列の行列をＭｄとすると、上記（３－７）は、下記（３－８）で示される。

【００４２】

【数２３】

$$\begin{array}{ll} \{M_d\}, & M_d : a \mapsto b_1 \\ \{M_d,\ M_d\}, & M_d^2 : a \mapsto b_2 \\ \{M_d,\ M_d,\ M_d\}, & M_d^3 : a \mapsto b_3 \\ \cdots\ \cdots\ \cdots & \cdots \\ \{M_d,\ M_d,\ M_d, \cdots, M_d\}, & M_d^k : a \mapsto b_k \end{array} \qquad (3\text{-}8)$$

【００４３】

上記ＯＰ$_1$ ～ＯＰ$_K$ によって規定される変換列の合成を表したｄｉ行ｍ列の行列Ｍｄ～Ｍｄ^k を縦に並べたｋ・ｄｉ×ｍの行列Ｍは、下記（３－９）で示される。

【００４４】

【数２４】

$$M := \begin{pmatrix} M_d \\ M_d^2 \\ \cdots \\ M_d^k \end{pmatrix} : a \mapsto \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_k \end{pmatrix} = \begin{pmatrix} D \cdot a \\ D^2 \cdot a \\ \cdots \\ D^k \cdot a \end{pmatrix} \qquad (3\text{-}9)$$

【００４５】

上記（３－９）に示すように、行列Ｍが、データａに対して第１の線形変換と、第２の変換Ｄ^2 ～Ｄ^k をそれぞれ行うｋ個の演算を規定している。

【００４６】

図７は、本実施形態の回路構成方法を実行するコンピュータ２９を説明するための図である。

図７に示すように、コンピュータ２９は、例えば、操作部３１、ディスプレイ３２、メモリ３３およびＣＰＵ３４を有し、これらがバス３０を介して接続されている。

操作部３１は、キーボードやマウスなどの操作手段であり、ＣＰＵ３４にプログラムの実行指示、データ選択指示、並びにデータ入力を行うために用いられる。

ディスプレイ３２は、ＣＰＵ３４の処理結果を表示する。

メモリ３３は、ＣＰＵ３４によって実行されるプログラム４１と、プログラム

４１の実行に用いられるデータ４２とを記憶する。

【００４７】

ＣＰＵ３４は、プログラム４１を実行して以下に示す処理を行い、プログラム４１の実行過程でデータ４２を用いて、演算回路１１の回路を構成（設計）する処理を行う。

プログラム４１は、本発明のプログラムに対応し、以下に示す各ステップの内容を示す手順を記述している。

また、ＣＰＵ３４がプログラム４１を実行することで、本発明の回路構成装置が構成され、ＣＰＵ３４がステップＳＴ１２を実行して本発明の第１の手段を構成し、ＣＰＵ３４がステップＳＴ１３を実行して本発明の第２の手段を構成する。

【００４８】

以下、本実施形態の回路構成方法の動作例を、ＣＰＵ３４の処理と関連付けて説明する。

図８は、本実施形態の回路構成方法の動作例を説明するためのフローチャートである。

ステップＳＴ１１：

ＣＰＵ３４は、例えば、ユーザによる操作部３１の操作に応じて、上記（３－４），（３－５），（３－６）に示すように演算回路１１が行う演算の入力および出力の形式、並びに上記（３－７）に示すように演算回路１１が行うそれぞれ所定の回数に対応する数の第１の線形変換Ｄをデータａに施す複数の演算の内容を規定するデータを入力する。

【００４９】

ステップＳＴ１２：

ＣＰＵ３４が、ステップＳＴ１１で入力した上記（３－７）に示す演算回路１１が行う複数の演算のそれぞれについて、上記所定の回数に対応する数の第１の線形変換Ｄを合成して得られる第２の線形変換（第１の演算）を行う上記（３－９）に示す行列Ｍを生成する処理を行う。

【００５０】

ステップＳＴ１３：

ＣＰＵ３４が、上記ステップＳＴ１２で規定された複数の第２の線形変換（第１の演算）を構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する。

〔００５１〕

ステップＳＴ１４：

ＣＰＵ３４が、複数の第２の線形演算（第１の演算）で共用されステップＳＴ１３で特定された上記第２の演算を行う第１の演算回路と、上記複数の第１の演算のそれぞれを構成する上記複数の第２の演算のうちステップＳＴ１３で特定された上記第２の演算以外の演算を行う第２の演算回路とからなる図９に示す演算回路１１を構成する。

このとき、ＣＰＵ３４が、上記（３－９）に示すステップＳＴ１２で生成された行列Ｍを基に、データＦＳ０に対して第１の線形変換Ｄ～D^k をそれぞれ行うｋ個の演算を並列に行うように演算回路１１の構成（設計）データを生成する。

具体的には、ＣＰＵ３４が、図９に示すように、データＦＳ０に対して第１の線形変換Ｄ～D^k をそれぞれ行う演算回路21_1 ～21_k を並列に配置した演算回路１１の構成を示す構成データを生成する。

〔００５２〕

これにより、ＣＰＵ３４は、入力したデータＦＳ０に上記（３－９）に示す行列Ｍで規定された線形変換を施し、データb_1 ～b_k を出力するように構成された演算回路１１の構成データを生成する。

〔００５３〕

図９に示すように演算回路１１を構成することで、レジスタ13_0 ～13_k からの出力は、横方向を時間として、図１０に示すようになる。

すなわち、演算回路１から、データb_1 ～b_k が略同じタイミングで出力されるため、データOUT_0 ～OUT_K も略同じタイミングで出力される。

このとき、演算回路１１が行う行列Ｍの演算と、演算回路１１に入力されるデータＦＳ０と、データOUT_0 ～OUT_K との関係は、下記（３－１０）で示される。

【００５４】

【数２５】

$$M \cdot FSO = \begin{pmatrix} D \cdot FSO \\ D^2 \cdot FSO \\ D^3 \cdot FSO \\ \vdots \\ D^K \cdot FSO \end{pmatrix} = \begin{pmatrix} OUT_0 \\ OUT_1 \\ OUT_2 \\ \vdots \\ OUT_k \end{pmatrix} \qquad (3-10)$$

【００５５】

ここで、上記行列Ｍは上記（３－１）で規定された線形空間の元によって構成されるため、データＯＵＴ$_1$～ＯＵＴ$_K$（データｂ$_1$～ｂ$_k$）は、上記線形空間の元とデータＦＳ０の各要素との積、並びにそれらの和として規定される。そのため、それらの組み合わせは、高々有限となり、例えば、値ｋが値ｍに対して大きい場合に、図８に示すように、演算回路１１から出力されたデータｂ$_k$を演算回路１４およびセレクタ１２を介して演算回路１１にフィーロバックすることで、多様な演算に対応可能な演算回路１１を小規模な構成で構築できる。

【００５６】

以下、ここで、図９に示す演算回路１１の演算回路２１$_1$，２１$_K$は、有限体Ｆ（2^4）の元、α，$\alpha^2+\alpha+1=0$に対してα倍演算を行なうものである場合、図１１に示す演算回路２２１のように構成される。

この場合に、図３に示すように、あるタイミングで入力されたデータａに対して、データＯＵＴ$_0$，ＯＵＴ$_1$，ＯＵＴ$_2$は、以下のようになる。

【００５７】

ＯＵＴ$_0$：ａ，$a\times\alpha^{k+1}$，$a\times\alpha^{2k+2}$，・・・，

ＯＵＴ$_1$：$a\times\alpha$，$a\times\alpha^{K+2}$，$a\times\alpha^{2K+3}$，・・・，

ＯＵＴ$_2$：$a\times\alpha^2$，$a\times\alpha^{K+3}$，$a\times\alpha^{2K+4}$，・・・，

すなわち、ＦＳ０＝Ａ０＋Ａ１αとすると、次のクロックサイクルにおけるデータＯＵＴ$_0$，ＯＵＴ$_1$，ＯＵＴ$_2$は、以下のようになる。

【００５８】

OUT_0 ：ＦＳ０＝Ａ０＋Ａ１α

OUT_1 ：ＦＳ０・α＝Ａ１＋（Ａ０＋Ａ１）α

OUT_2 ：ＦＳ０・α・α＝（Ａ０＋Ａ１）＋Ａ０α

〔００５９〕

この場合に、前述した図８に示すステップＳＴ１３において、ＣＰＵ３４が、上記α倍演算を構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う上記第２の演算、すなわち、演算「Ａ０＋Ａ１」を特定する。

そして、図８に示すステップＳＴ１４において、ＣＰＵ３４が、複数のα倍演算（すなわち、α倍演算と、α^2倍演算）で共用されステップＳＴ１３で特定された演算「Ａ０＋Ａ１」を行う図１１に示す第１の演算回路１１５（図１１では加算回路）と、複数のα倍演算のそれぞれを構成する上記複数の第２の演算のうちステップＳＴ１３で特定された上記第２の演算以外の演算を行う第２の演算回路（図１１に示す例では無し）とからなる図１１に示す演算回路１１ａを構成する。

〔００６０〕

なお、上述した実施形態において、上記第１の線形変換が、上記（３－１）で規定した線形空間の元γに対してγ^r倍演算（$\times\gamma^r$）を行うものである場合には、上記複数の演算を、それぞれOP_1～OP_Kとすると、これらは下記（３－１１）で示される。

〔００６１〕

【数２６】

$$
\begin{array}{lllll}
OP_1: & \{(\times\gamma')\}, & & (\times\gamma'): & a \mapsto b_1 \\
OP_2: & \{(\times\gamma'),\ (\times\gamma')\}, & & (\times\gamma')\circ(\times\gamma'): & a \mapsto b_2 \\
OP_3: & \{(\times\gamma'),\ (\times\gamma'),\ (\times\gamma')\}, & & (\times\gamma')\circ(\times\gamma')\circ(\times\gamma'): & a \mapsto b_3 \\
 & \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots & & \cdots & \cdots \\
OP_k: & \{(\times\gamma'),\ (\times\gamma'),\ (\times\gamma'),\cdots,(\times\gamma')\}, & & (\times\gamma')\circ(\times\gamma')\circ(\times\gamma')\circ\cdots\circ(\times\gamma')\circ: & a \mapsto b_k
\end{array}
$$

(3-11)

〔００６２〕

そして、第１の線形変換Ｄを表すｄｉ行ｍ列の行列をＭｒとすると、上記（３－１１）は、下記（３－１２）で示される。

【００６３】

【数２７】

$$\begin{array}{ll} \{M_r\}, & M_r : a \mapsto b_1 \\ \{M_r,\ M_r\}, & M_r^2 : a \mapsto b_2 \\ \{M_r,\ M_r,\ M_r\}, & M_r^3 : a \mapsto b_3 \\ \cdots\ \cdots\ \cdots\ \cdots & \cdots \\ \{M_r,\ M_r,\ M_r,\ \cdots, M_r\}, & M_r^k : a \mapsto b_k \end{array} \qquad (3\text{-}12)$$

【００６４】

上記ＯＰ$_1$～ＯＰ$_K$によって規定される変換列の合成を表したｄｉ行ｍ列の行列Ｍｒ～Ｍｒ^{k}を縦に並べたｋ・ｄｉ×ｍの行列Ｍｒは、下記（３－１３）で示される。

ここで、Ｍｒ^x（ｘは１≦ｘ≦ｋを満たす整数）は、Ｘ個のＭｒを合成した行列である。

【００６５】

【数２８】

$$M := \begin{pmatrix} M_r \\ M_r^2 \\ \cdots \\ M_r^k \end{pmatrix} : a \mapsto \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_k \end{pmatrix} = \begin{pmatrix} \gamma^r \cdot a \\ \gamma^{2r} \cdot a \\ \cdots \\ \gamma^{kr} \cdot a \end{pmatrix} \qquad (3\text{-}13)$$

【００６６】

上記（３－１３）に示すように、行列Ｍが、データａに対してγ^r～r^{kr}倍演算（×γ^r）をそれぞれ行うｋ個の演算を規定している。

【００６７】

この場合には、図１２に示すように、ＣＰＵ３４が、データＦＳ０に対してγ^r～r^{kr}倍演算（×γ^r）をそれぞれ行う演算回路２１$_1$～２１$_k$を有する演算回路１１の構成を示す構成データを生成する。

【００６８】

以上説明したように、本実施形態の回路構成方法では、上述したように図８に示すステップＳＴ１３において、複数の第１の演算（Ｄ倍演算、α倍演算）を構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う上記第２の

演算を特定する。

そして、ステップＳＴ１４において、上記複数の第１の演算で共用され上記特定された上記第２の演算を行う第１の演算回路と、上記複数の第１の演算のそれぞれを構成する上記複数の第２の演算のうち上記特定された上記第２の演算以外の演算を行う第２の演算回路とからなる演算回路１１，１１ａを構成する。

そのため、本実施形態の回路構成方法によれば、演算回路１１，１１ａを小規模に構成できる。

【００６９】

また、本実施形態の回路構成方法では、図８に示すステップＳＴ１２で、ステップＳＴ１１で入力した上記（３－７）に示す演算回路１１が行う複数の演算のそれぞれについて、上記所定の回数に対応する数の第１の線形変換Ｄを合成して得られる第２の線形変換（第１の演算）を行う上記（３－９）に示す行列Ｍを生成し、これに対して上述したステップＳＴ１３，ＳＴ１４の処理を行う。

そのため、本実施形態の回路構成方法によれば、演算回路１１，１１ａを小規模に構成できると共に、演算時間を短縮できる。

また、本実施形態の回路構成方法では、図９および図１１に示すように、演算回路１１が、データＦＳ０に対して、第１の演算を並列に行うため、演算時間をさらに短縮できる。

すなわち、演算回路21_1～21_kにおいてデータＦＳ０（データａ）を並列に処理するため、データb_1～b_k（データOUT_1～OUT_K）の全てを略同じタイミングで得ることができる。

そのため、データＦＳ０を入力してからデータb_2～b_kを得るまでの時間を図３に示す構成に比べて短縮した演算回路１１を構成（設計）できる。

【００７０】

〔第２実施形態〕

本実施形態では、有限体Ｆ（2^4）上の元として扱われる４ビットのデータＤ（＝Ｄ〔３〕，Ｄ〔２〕，Ｄ〔１〕，Ｄ〔０〕）を縦ベクトルと見なし、当該データＤに対して下記（３－１４），（３－１５）で示す行列Ｍ１，Ｍ２で示される２つの線形変換を施す回路を構成する場合を例示する。

【００７１】

【数２９】

$$M1 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad (3-14)$$

【００７２】

【数３０】

$$M2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad (3-15)$$

【００７３】

従来では、出力値Ｅ１＝Ｍ１・Ｄ、Ｅ２＝Ｍ２・Ｄは、それぞれ縦ベクトルとして表現され、下記（３－１６），（３－１７）で示される。

【００７４】

【数３１】

$$E1=(E1[3],E1[2],E1[1],E1[0]$$
$$=(D[1]+D[2],D[3],D[0]+D[2],D[0]+D[1]+D[3]) \qquad (3-16)$$

【００７５】

【数３２】

$$E2=(E2[3],E2[2],E2[1],E2[0]$$
$$=(D[1],D[0],D[0]+D[2]+D[3],D[1]+D[2]) \qquad (3-17)$$

【００７６】

従来の回路構成方法では、図１３に示すように、上記（３－１６）に示す演算を行う演算回路４０２と、上記（３－１７）に示す演算を行う演算回路４０３とを有する演算回路４０１が構成される。

演算回路４０２は、加算回路４１１，４１２，４１３，４１４で構成される。

また、演算回路４０３は、加算回路４２１，４２２，４２３で構成される。

【００７７】

本実施形態の回路構成方法は、上記（３－１４），（３－１５）に示す行列Ｍ

１，Ｍ２によって表現される線形変換を，有限体Ｆ（2^4）上の元として扱われる４ビットのデータＤ（＝Ｄ〔３〕，Ｄ〔２〕，Ｄ〔１〕，Ｄ〔０〕）に施すことは同じである。

本実施形態では、２つの４×４行列を用いる代わりに、行列Ｍ１とＭ２とを連結した下記（３－１８）に示される行列Ｍを用いる。

【００７８】

【数３３】

$$M = \begin{pmatrix} M1 \\ M2 \end{pmatrix} = \begin{pmatrix} 1\,1\,0\,1 \\ 1\,0\,1\,0 \\ 0\,0\,0\,1 \\ 0\,1\,1\,0 \\ 0\,1\,1\,0 \\ 1\,0\,1\,1 \\ 1\,0\,0\,0 \\ 0\,1\,0\,0 \end{pmatrix} \qquad (3\text{-}18)$$

【００７９】

本実施形態の回路構成方法では、上記行列Ｍの演算を行い、上記（３－１６），（３－１７）内の演算において、行列Ｍ１に相当する第１の演算と行列Ｍ２に相当する第１の演算とを構成する複数の第２の演算のうち、共通する第２の演算である「Ｄ〔０〕＋Ｄ〔２〕」、並びに「Ｄ〔１〕＋Ｄ〔２〕」を特定する。

そして、図１４に示すように、第２の演算「Ｄ〔０〕＋Ｄ〔２〕」を行う図１３に示す加算回路４１２と４２１と、第２の演算「Ｄ〔１〕＋Ｄ〔２〕」を行う図１３に示す加算回路４１３と４２２が共用化され、加算回路４１２，４１３が削減され、図１３に示す演算回路４０１に比べて、回路規模が縮小された演算回路４０３が構成される。

これにより、図１３に示す演算回路４０１と同じ演算を行う図１４に示す演算回路４０３を、演算回路４０１に比べて小規模に構成できる。

【００８０】

本発明は上述した実施形態には限定されない。

その他の実施形態として、上記所定の基底として下記（３－１９）に示す基底を用い、上記データａを下記（３－２０）のように示し、前記データａをｍ次元

ベクトルとして下記（３－２１）のように示してもよい。

【００８１】

【数３４】

$$\{1, \gamma, \gamma^2, \cdots, \gamma^{m-1}\} \qquad (3-19)$$

【００８２】

【数３５】

$$a = a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3 + \cdots + a_{m-1}\gamma^{m-1} \qquad (3-20)$$

【００８３】

【数３６】

$$a = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{m-1} \end{pmatrix} \qquad (3-21)$$

【００８４】

【発明の効果】

以上説明したように、本発明によれば、所定データに対してそれぞれ異なる複数の演算を行なう演算回路を構成する場合に、当該演算回路を小規模に構成できる回路構成方法、その装置およびそのプログラムを提供することができる。

【図面の簡単な説明】

【図１】

図１は、本発明の関連技術を説明するための図である。

【図２】

図２は、本発明の関連技術を説明するための図である。

【図３】

図３は、本発明の関連技術を説明するための図である。

【図４】

図４は、本発明の関連技術を説明するための図である。

【図５】

図５は、本発明の関連技術を説明するための図である。

【図６】

図６は、本発明の第１実施形態の回路構成方法で構成（設計）される演算回路の周辺回路を説明するための図である。

【図７】

図７は、本発明の第１実施形態の回路構成方法を実行するコンピュータを説明するための図である。

【図８】

図８は、本発明の第１実施形態の回路構成方法の手順によって演算回路を構成する場合を説明するためのフローチャートである。

【図９】

図９は、本発明の第１実施形態の回路構成方法で構成（設計）される演算回路を説明するための図である。

【図１０】

図１０は、図９に示す演算回路のデータ出力タイミングを説明するための図である。

【図１１】

図１１は、図９に示す演算回路の具体例を説明するための図である。

【図１２】

図１２は、本発明の第１実施形態の回路構成方法によって構成されるγ^{r}～r^{kr}倍演算（×γ^{r}）を行う演算回路を説明するための図である。

【図１３】

図１３は、本発明の第２実施形態の回路構成方法の関連技術を説明するための図である。

【図１４】

図１４は、本発明の第２実施形態の回路構成方法を説明するための図である。

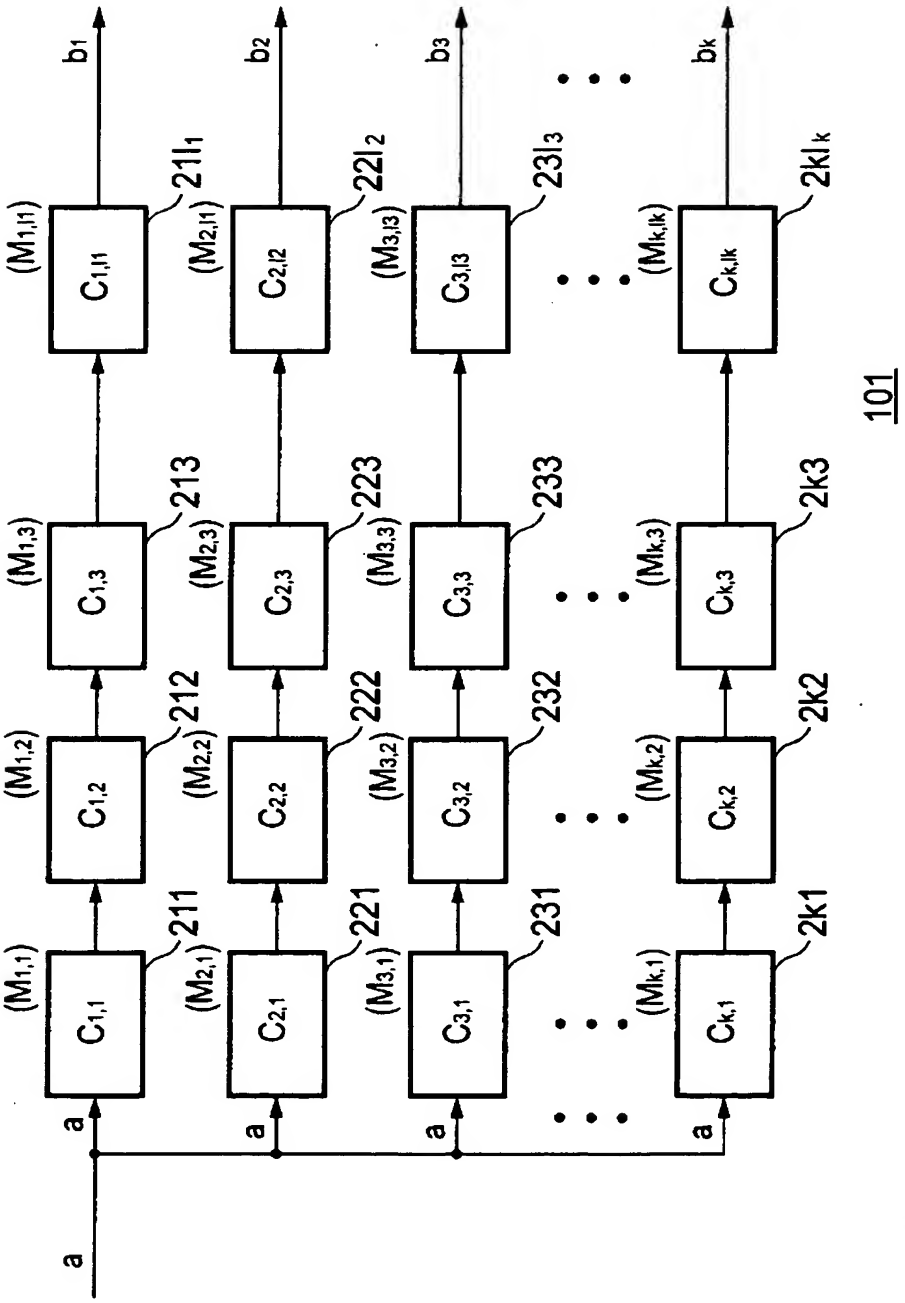
【符号の説明】

１１…演算回路、１２…セレクタ、13_0～13_k…レジスタ、１４…演算回路、21_1～21_k…演算回路、３０…バス、３１…操作部、３２…ディスプレ

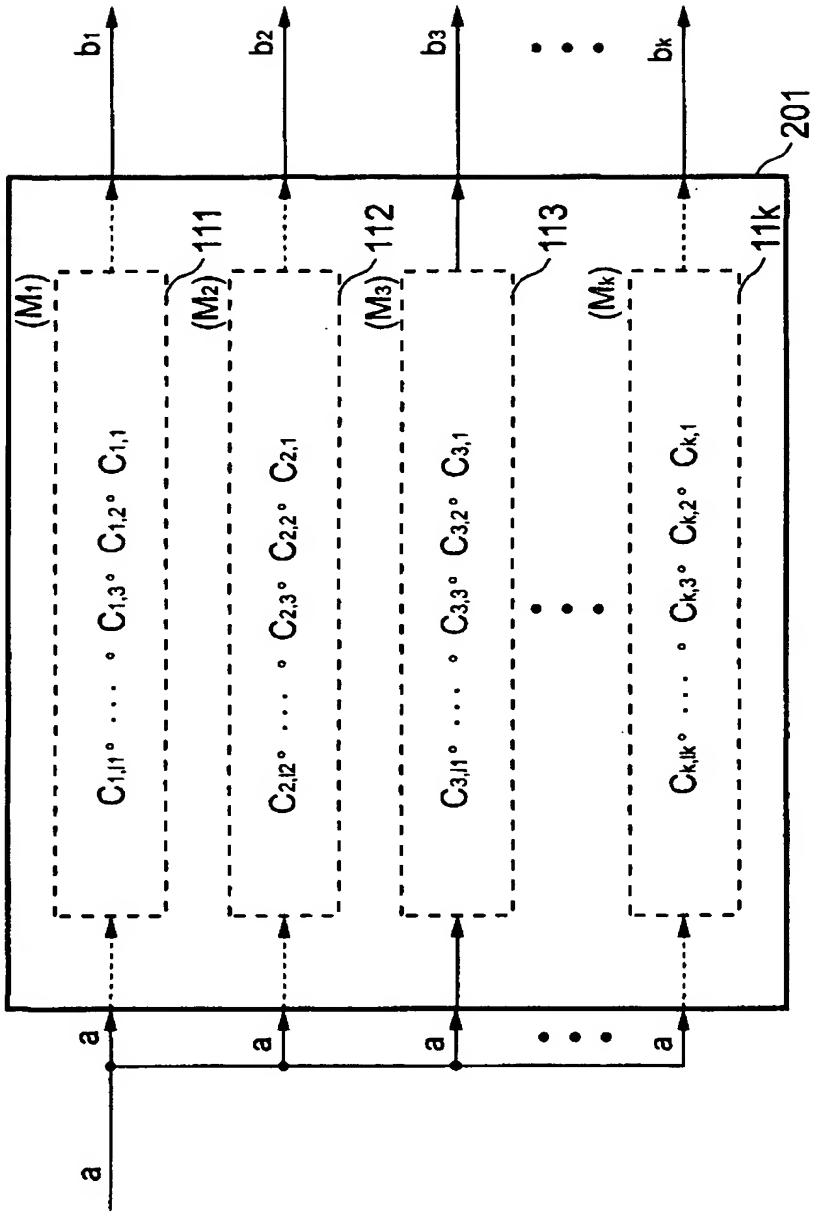
イ、３３…メモリ、４１…プログラム、４２…データ

【書類名】　図面

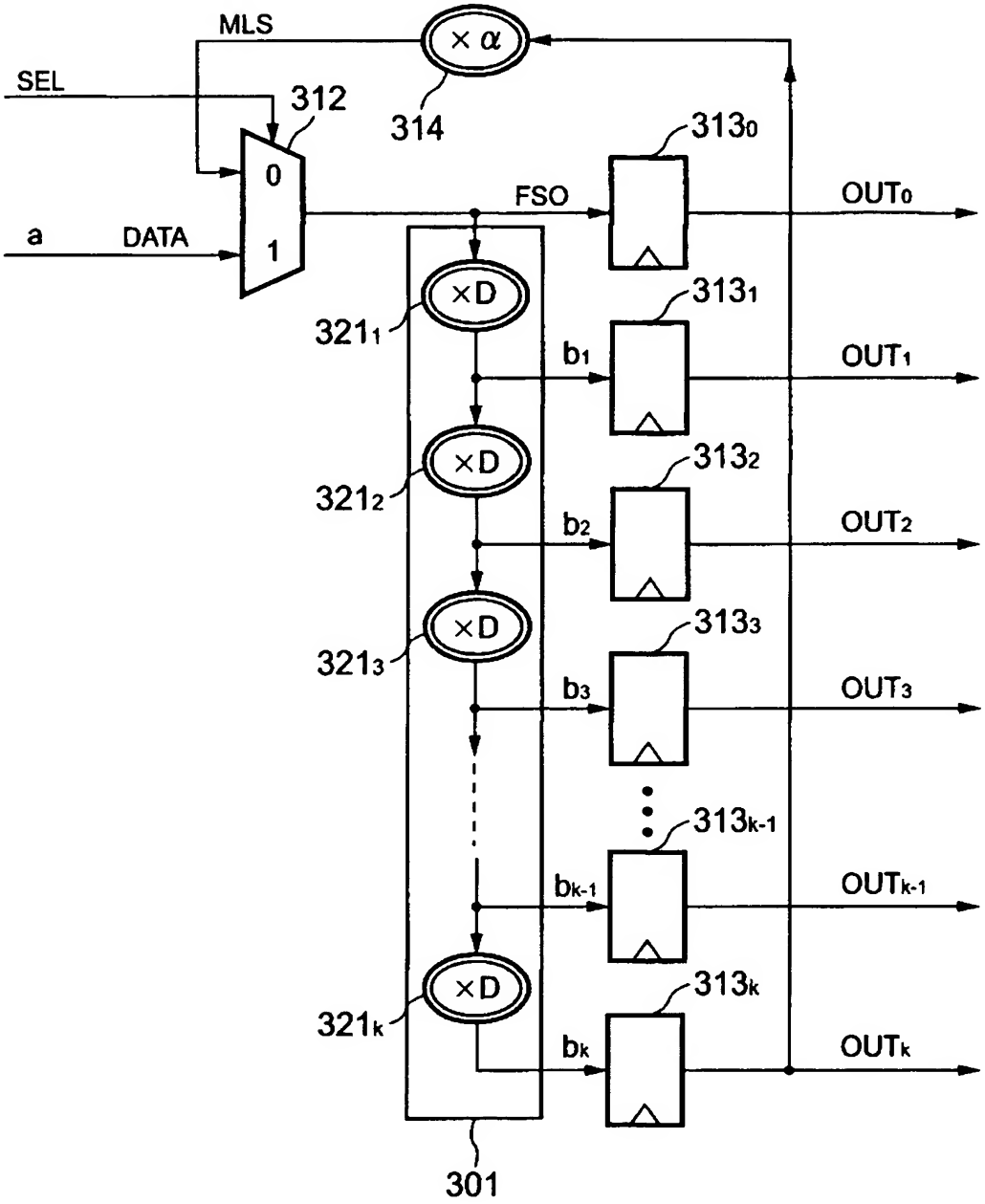
【図１】



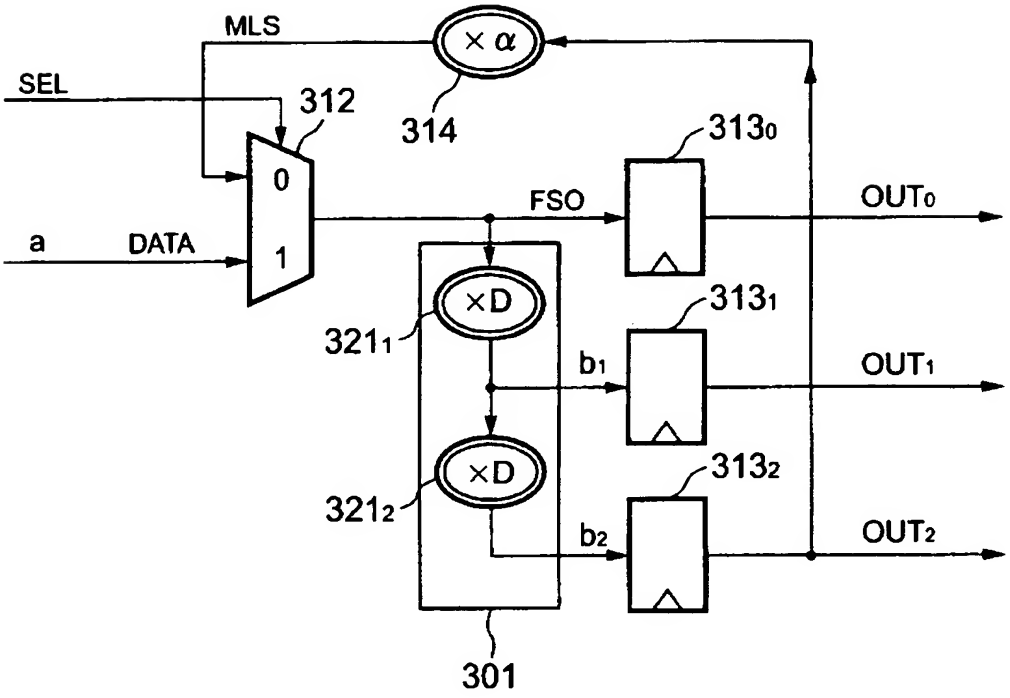
【図２】


b1
b2
b3
bk
201
111
112
113
11k
(M1)
(M2)
(M3)
(Mk)
C1,I1° ... ° C1,3° C1,2° C1,1
C2,I2° ... ° C2,3° C2,2° C2,1
C3,I1° ... ° C3,3° C3,2° C3,1
Ck,Ik° ... ° Ck,3° Ck,2° Ck,1
a
a
a
a
a

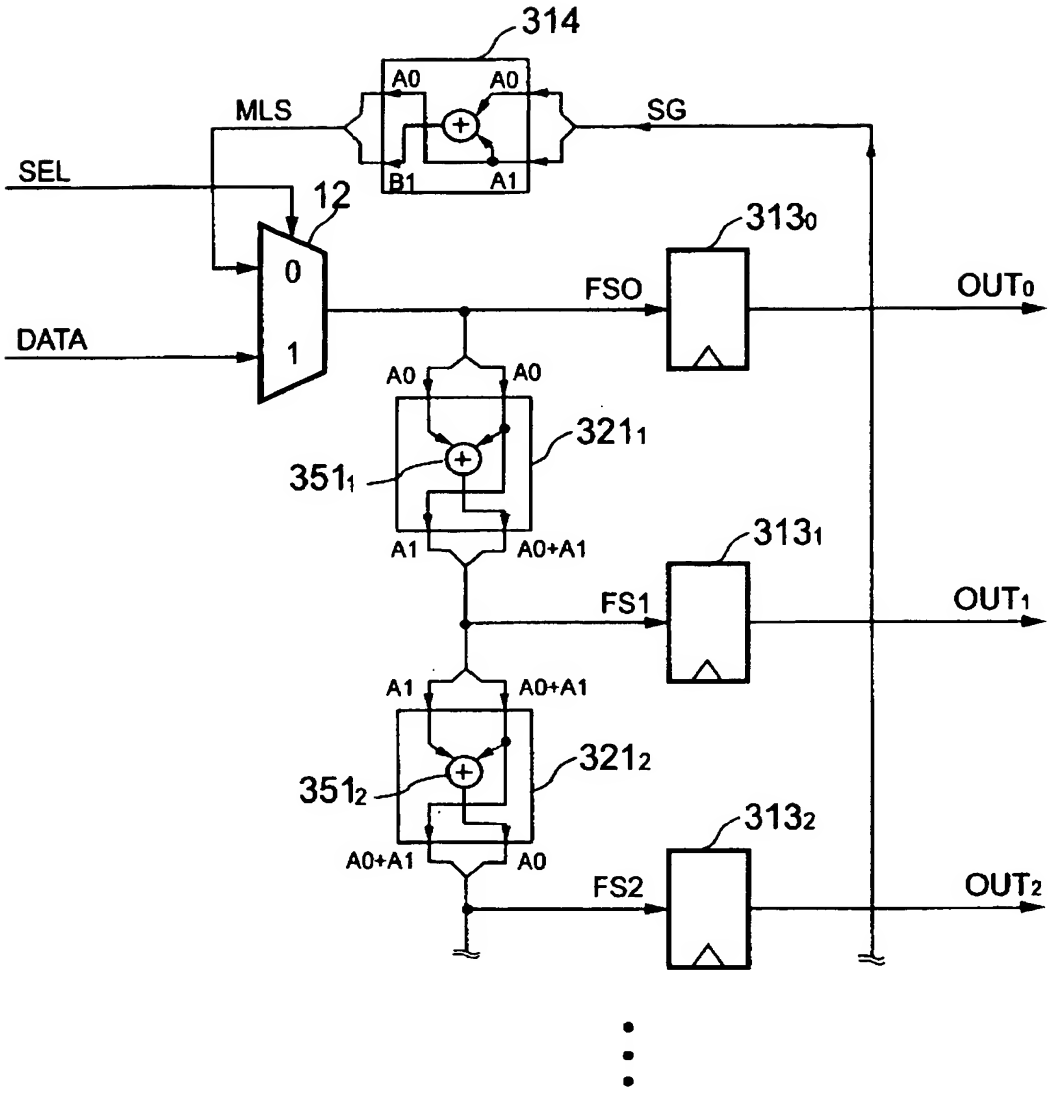
【図３】


MLS
×α
SEL
312
314
313₀
0
FSO
OUT₀
a
DATA
1
×D
321₁
313₁
b₁
OUT₁
×D
321₂
313₂
b₂
OUT₂
×D
321₃
313₃
b₃
OUT₃
313k-1
bk-1
OUTk-1
×D
321k
313k
bk
OUTk
301

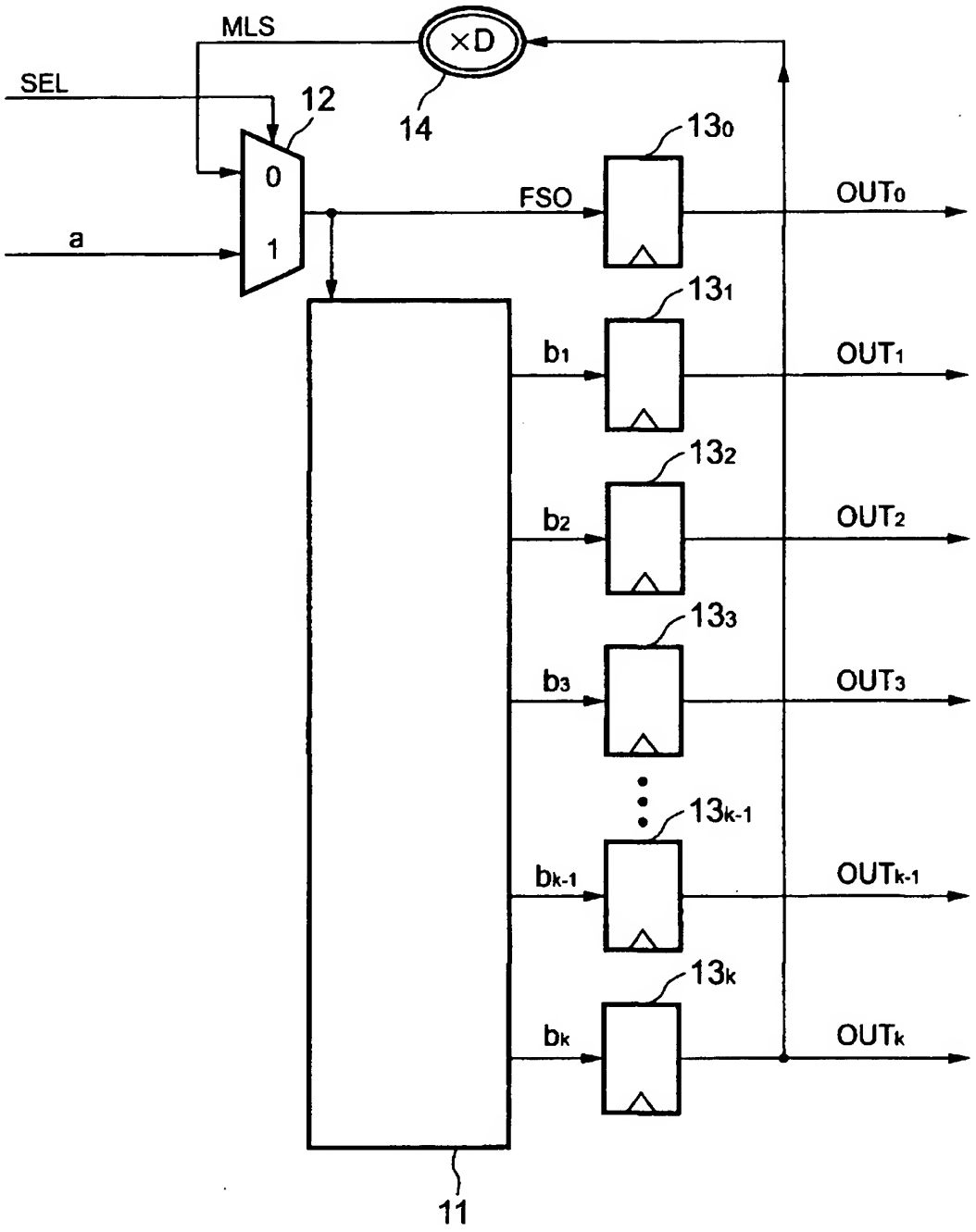
【図４】


MLS
×α
SEL
312
314
313₀
0
FSO
OUT₀
a
DATA
1
×D
321₁
313₁
b₁
OUT₁
×D
321₂
313₂
b₂
OUT₂
301

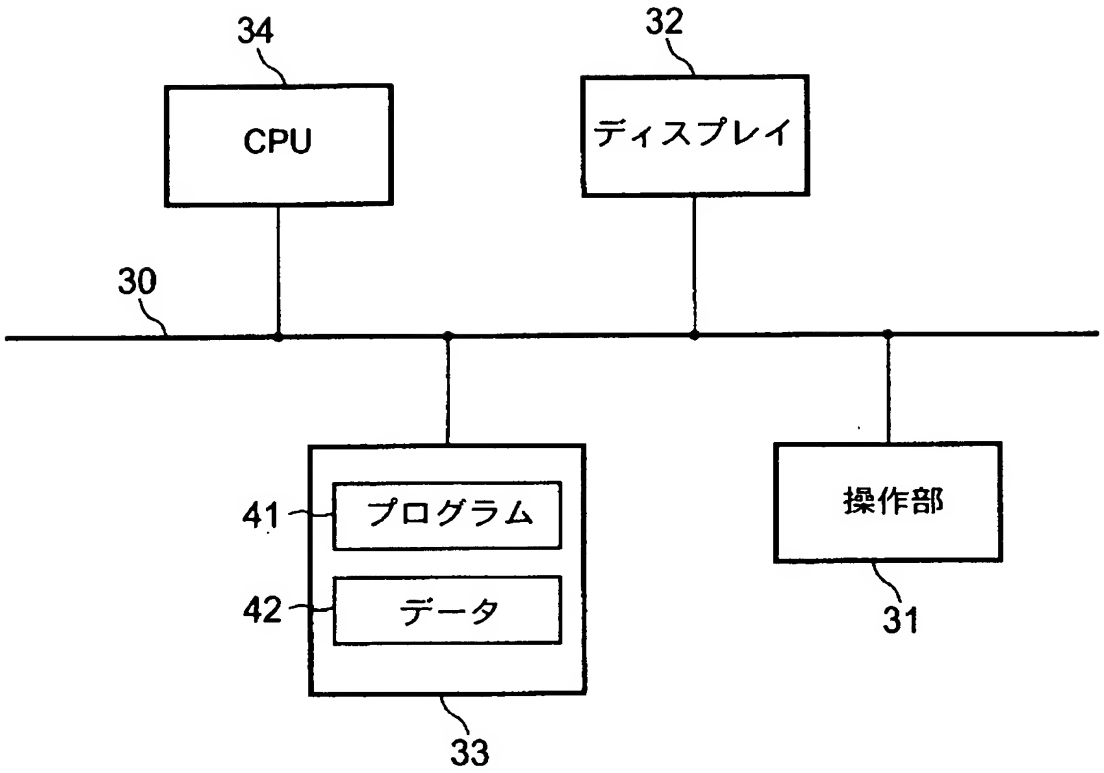
【図５】


314
A0
A0
MLS
SG
B1
A1
SEL
12
0
1
DATA
313₀
FSO
OUT₀
A0
A0
321₁
351₁
A1
A0+A1
313₁
FS1
OUT₁
A1
A0+A1
321₂
351₂
A0+A1
A0
313₂
FS2
OUT₂

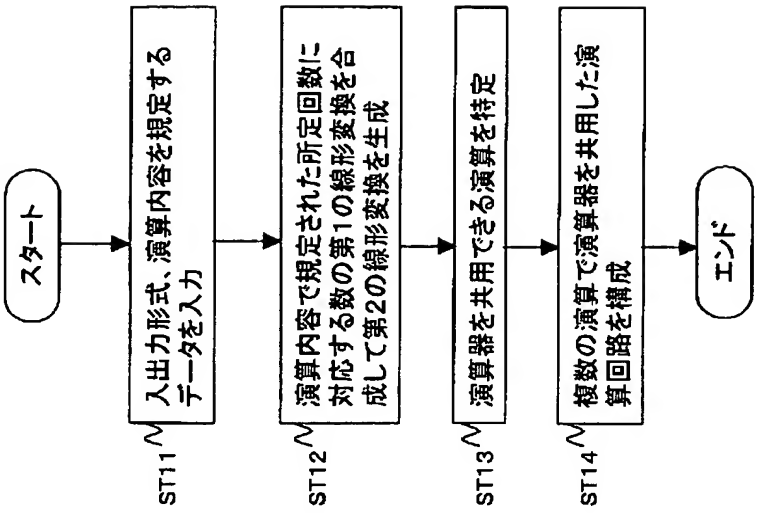
【図６】


MLS
×D
SEL
12
14
130
0
FSO
OUT0
a
1
131
b1
OUT1
132
b2
OUT2
133
b3
OUT3
13k-1
bk-1
OUTk-1
13k
bk
OUTk
11

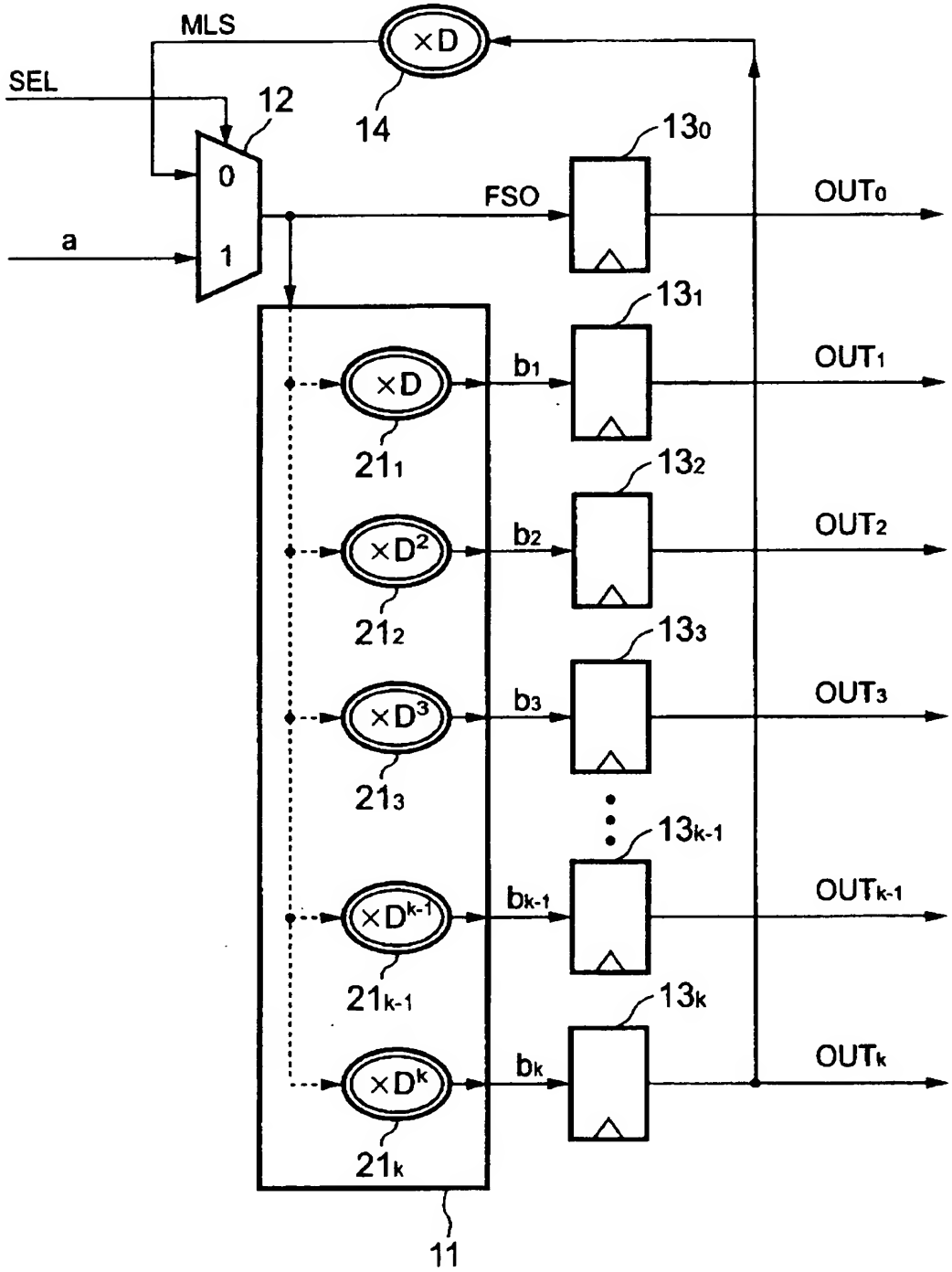
【図７】



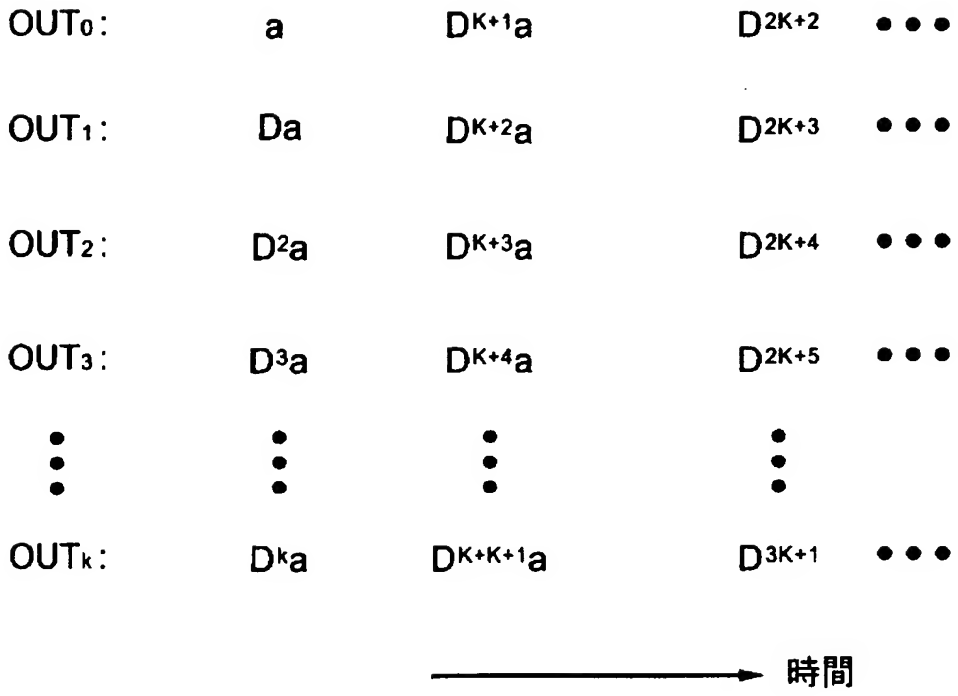
【図８】


スタート
入出力形式、演算内容を規定するデータを入力
ST11
演算内容で規定された所定回数に対応する数の第1の線形変換を合成して第2の線形変換を生成
ST12
演算器を共用できる演算を特定
ST13
複数の演算で演算器を共用した演算回路を構成
ST14
エンド

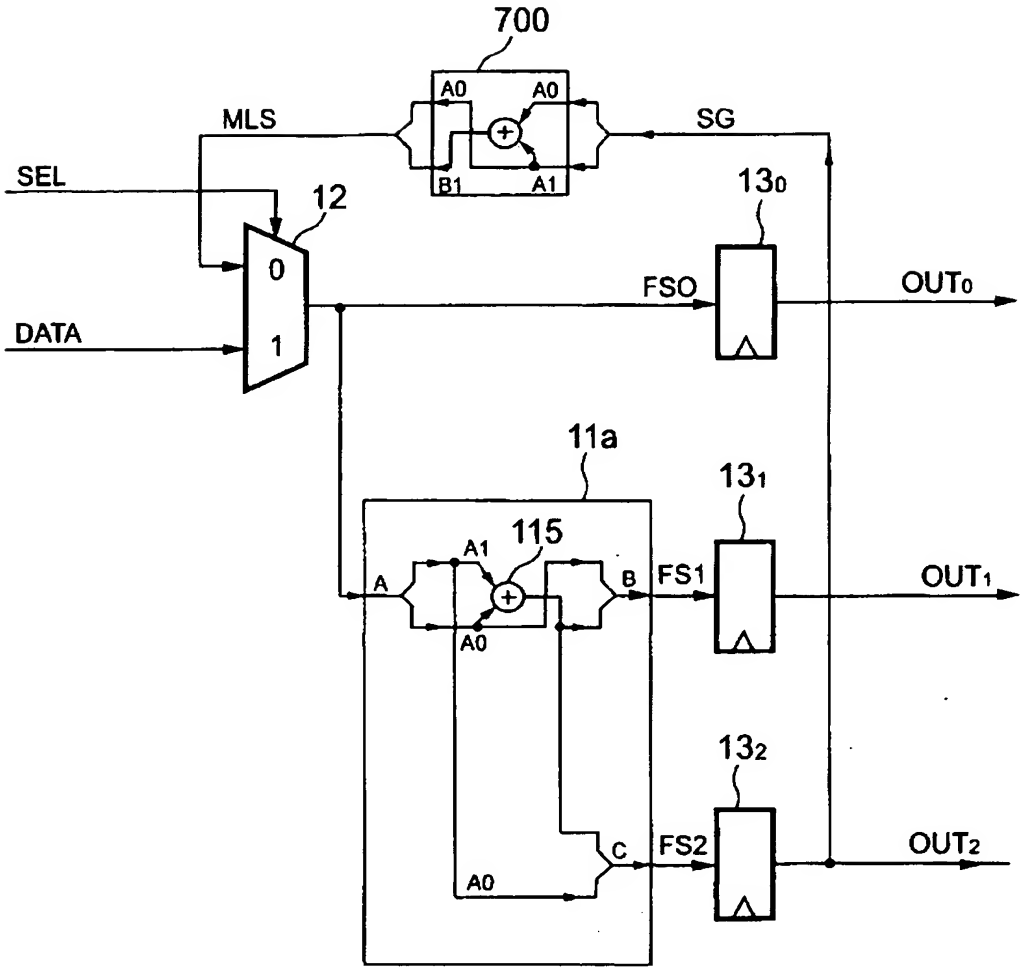
【図９】


MLS
×D
14
SEL
12
0
1
a
FSO
13₀
OUT₀
13₁
OUT₁
b₁
×D
21₁
13₂
OUT₂
b₂
×D²
21₂
13₃
OUT₃
b₃
×D³
21₃
13k-1
OUTk-1
bk-1
×Dk-1
21k-1
13k
OUTk
bk
×Dk
21k
11

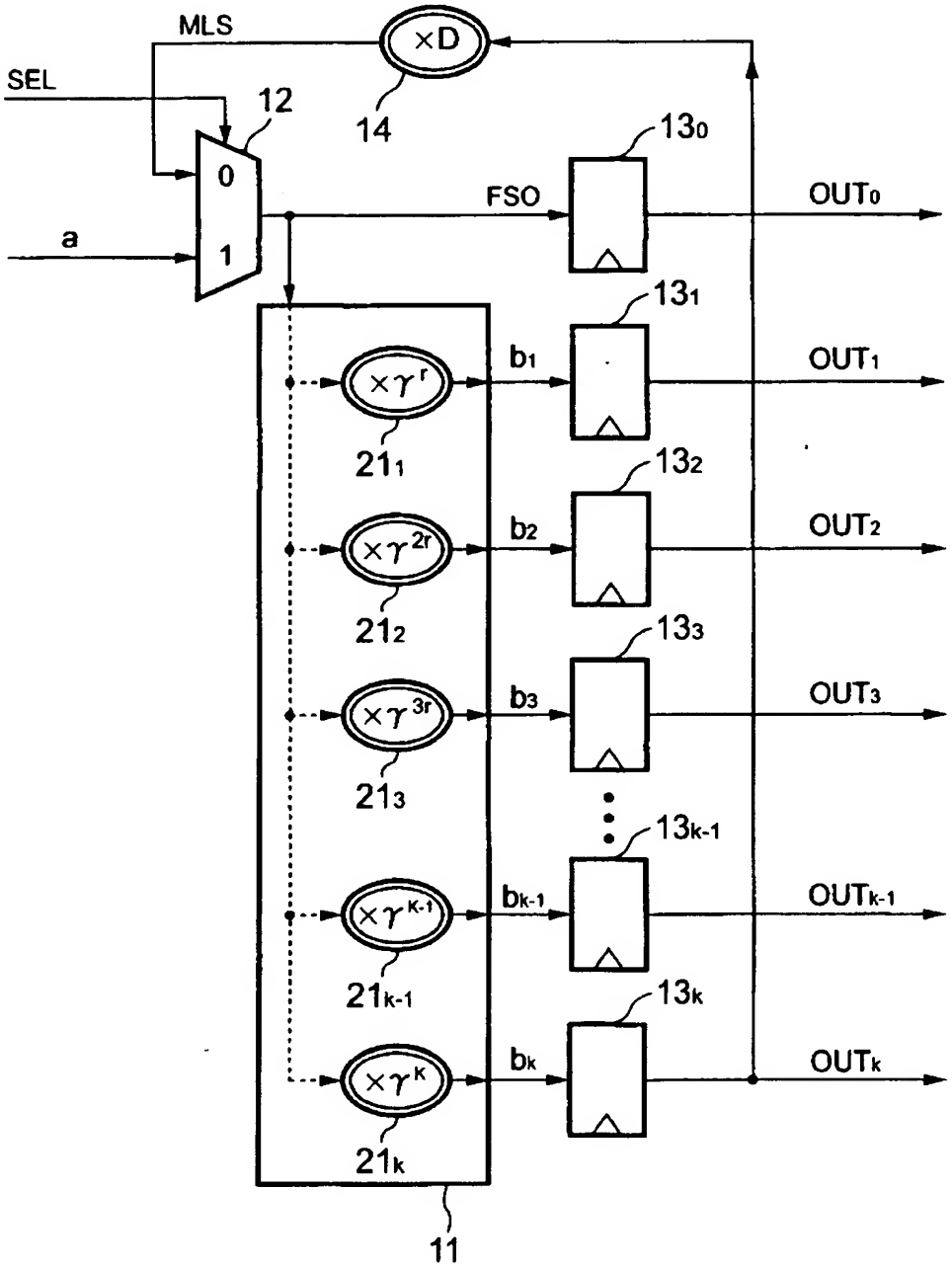
【図１０】


OUT0:
a
DK+1a
D2K+2
OUT1:
Da
DK+2a
D2K+3
OUT2:
D2a
DK+3a
D2K+4
OUT3:
D3a
DK+4a
D2K+5
OUTk:
Dka
DK+K+1a
D3K+1
時間

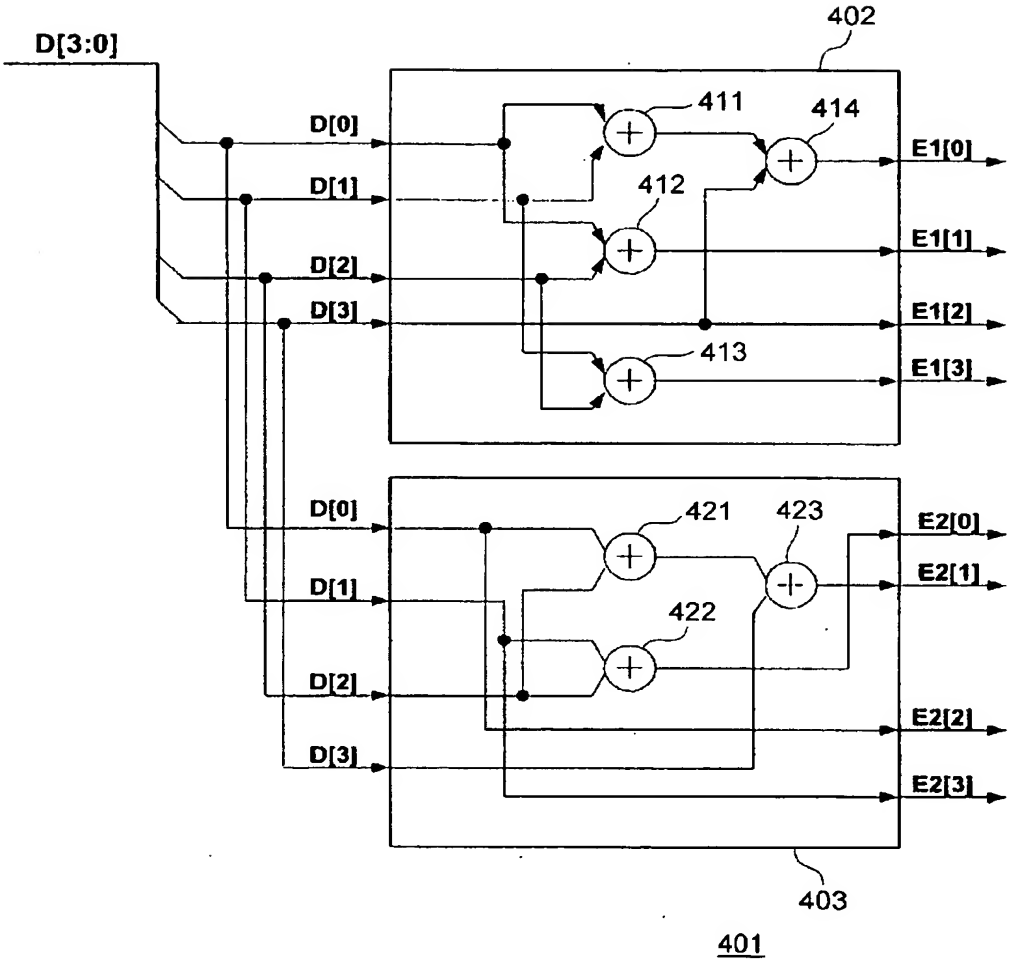
【図１１】


700
A0
A0
B1
A1
MLS
SG
SEL
12
0
1
DATA
FSO
13_0
OUT_0
11a
115
A1
A
B
A0
FS1
13_1
OUT_1
13_2
C
FS2
OUT_2
A0

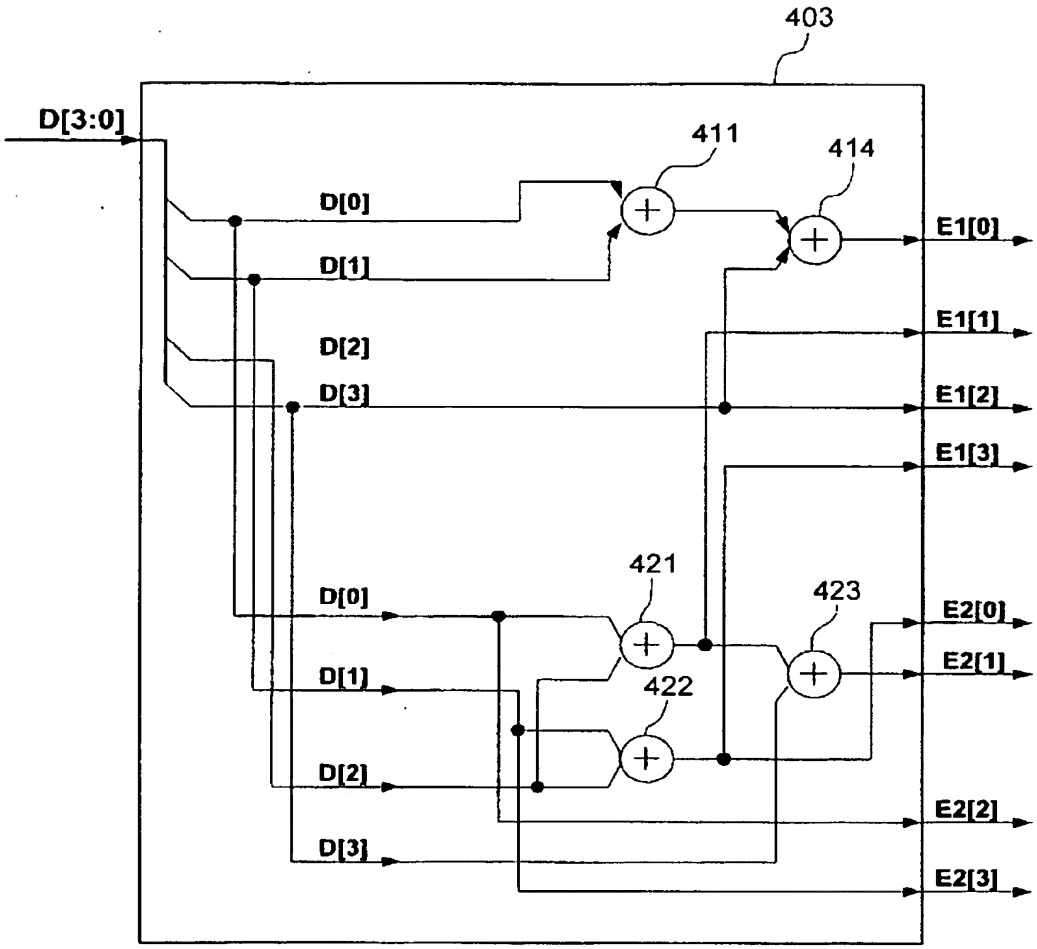
【図１２】


MLS
×D
SEL
12
14
0
1
a
FSO
13_0
OUT_0
13_1
b_1
OUT_1
21_1
13_2
b_2
OUT_2
21_2
13_3
b_3
OUT_3
21_3
13_{k-1}
b_{k-1}
OUT_{k-1}
21_{k-1}
13_k
b_k
OUT_k
21_k
11

【図１３】


D[3:0]
402
D[0]
D[1]
D[2]
D[3]
411
412
413
414
E1[0]
E1[1]
E1[2]
E1[3]
D[0]
D[1]
D[2]
D[3]
421
422
423
E2[0]
E2[1]
E2[2]
E2[3]
403
401

【図１４】


403
D[3:0]
411
414
D[0]
D[1]
D[2]
D[3]
E1[0]
E1[1]
E1[2]
E1[3]
421
423
422
D[0]
D[1]
D[2]
D[3]
E2[0]
E2[1]
E2[2]
E2[3]

【書類名】　　要約書

【要約】

【課題】　所定データに対してそれぞれ異なる複数の演算を行なう演算回路を構成する場合に、当該演算回路を小規模に構成できる回路構成方法を提供する。

【解決手段】　所定のデータに対してそれぞれ異なる複数の第１の演算を施す演算回路を設計する場合に、複数の第１の演算のそれぞれを構成する複数の第２の演算のうち、同じデータに対して同じ演算を行う前記第２の演算を特定する（ＳＴ１３）。そして、複数の第１の演算で共用されＳＴ１３で特定された第２の演算を行う演算回路を有する演算回路を構成する（Ｔ１４）。

【選択図】　図８

特願２００２－３３１６７７

出　願　人　履　歴　情　報

識別番号　　［０００００２１８５］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社